Weekly Report

Junming Ke(2017.05.01-2017.05.07)

Recently, I have already read a lot of papers about Blockchain, and have prepared for the presentation in Information Security class. The details are as follows:

Papers

SOK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
This is a survey paper presented by Joseph Bonneau and Andrew Miller published in IEEE Symposium on Security and Privacy. This paper provide a depth introduction about Bitcoin, and analyse the property of Bitcoin very closely, Furthermore, they have identify the challenges atop the blockchain. Many people believe this paper is the first authority survey among blockchain area.

Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies
Published in IEEE Communications Survey & Tutorials. And we believe it's the second powerful survey among the blockchain field, Comparatively speaking, this article is more detailed, which means this article provide a widely introduction about blockchain. From the beginning, this article introduce the history and properties about blockchain briefly. Then it conduct a discussion about the properties about blockchain, more detailed. Indeed, I have focus on VI chapter which is about PROOF-OF-X(POX) SCHEMES. And conclude as follows:

目前电子货币采用的共识类型

共识类型	简要介绍	应用实例
POW 工作量证明	POW 主要是依赖机器进行数学运算来获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网 50%节点出错。	B-money， Karma，RPOW， Bit Gold，Litecoin， Dogecoin，MAVEPAY，FawkesCoin
POS 股权证明	主要思想是节点记账权的获得难度与节点持有的权益成反比，相对于 PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和 PoW 相同。	Nextcoin，PPCoin
POA 活跃度证明	POA 挖矿过程与 POW 类似，在增加区块时，系统会选择在线人数进行奖励，这种操作有利于减少线下收藏的情况，鼓励线上活跃节	Reddcoin，BitTorrent

	点。	
POB 摧毁证明	应用安全多方计算知识，矿工必须证明他们摧毁了一些原有的币，这将有利于解决分叉问题，同时可以应用在侧链等问题上。类似的还有带宽证明和可回收性证明。	Counterparty，Mastercoin，Permacoin
中心化指定权限	这种方式是采用中心化的思想，如果我们可以相信一小部分拥有指定权限的人群，那么所有的共识问题都将变得简单。	R3

Furthermore, I also have read:
Summary of the confidentially and privacy report.pdf
On scaling decentralized blockchains.pdf
R3 confidentially and privacy report.pdf
However, I don't read these paper carefully, just know what the main work is.

Presentation

This week I have presented the article:
Stealing Machine Learning Models via Prediction APIs.
In the Information Security class.

Next week

1. Go to Sansec company for work internship, and practice Hyperledger project.
2. Following articles:
   Secure Multiparty Computations on Bitcoin
   How to Use Bitcoin to Design Fair Protocols
3. Business plan homework;
   Data mining group presentation;
   Information security review;
   Visualization project;
   English writing class formulate conference submission.
4. LaTex
   Docker
   Git
   Linux